

AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph [0051], with the following marked-up version of the paragraph:

[0051] Generally, encrypted data sent between client side 350 and server side 360 is encrypted using a tunnel key. The tunnel key can be derived by hashing the concatenation of a Diffie-Hellman shared secret (e.g., session key ~~[[344]]~~131) together with client and server nonces. For example, a tunnel key can be derived according to the following formula:

$$\text{Tunnel Key} = \text{HASH} [\text{DH}_{ss} + N_c + N_s]$$

Please replace the paragraph [0053], with the following marked-up version of the paragraph:

[0053] When client side 350 and server side 360 are performing a negotiation, server request 313 can include negotiation encrypted content 318. Negotiation encrypted content 318 can include challenge 319, authentication method 321, and trust anchor 322. Challenge 319 can be an HMAC of the previous packet ID (e.g., pervious packet ID 314) using a shared secret (e.g., session key ~~[[344]]~~131). For example, challenge 319 can be configured according to the following formula:

$$\text{Challenge} = \text{HMAC}_{ss}[\text{PPid}]$$